

О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫЕ СЕТИ [сетевые аномалии]

Под редакцией профессора О. И. Шелухина

*Рекомендовано УМО по образованию в области
Инфокоммуникационных технологий и систем связи в качестве
учебного пособия для студентов высших учебных заведений,
обучающихся по направлению подготовки
210700 - «Инфокоммуникационные технологии и системы связи»
квалификации (степени) «бакалавр» и «магистр»*

**Москва
Горячая линия - Телеком
2013**

УДК 004.732.056(075.8)

ББК 32.973.2-018.2я73

Ш44

Рецензенты: доктор техн. наук, профессор, академик РАЕН, декан факультета «Кибернетика и информационная безопасность НИЯУ МИФИ» *С. В. Дворянкин*, доктор техн. наук, профессор, зав. кафедрой «Информационная безопасность телекоммуникационных систем» ЮФУ *К. Е. Румянцев*, доктор техн. наук, профессор кафедры «Информационная безопасность и автоматизация» МТУСИ *С. С. Звездинский*, канд. техн. наук, доцент кафедры «Информационная безопасность» МГТУ им Н. Э. Баумана *Р. А. Бельфер*,

Шелухин О. И., Сакалема Д. Ж., Филинова А. С.

Ш44 Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов. / Под ред. профессора О. И. Шелухина – М.: Горячая линия–Телеком, 2013. – 220 с: ил. ISBN 978-5-9912-0323-4.

Даны основные определения и понятия в области систем обнаружения вторжений и компьютерных атак. Рассмотрены принципы построения и структура систем обнаружения вторжений. Анализируются способы развертывания, достоинства и недостатки существующих систем обнаружения вторжений. Центральное место в книге уделено методам обнаружения сетевых аномалий. Рассмотрены методы кратномасштабного вейвлет- и мультифрактального анализа алгоритмов обнаружения аномальных вторжений. Проведен анализ статистических, интеллектуальных, иммунных, нейросетевых и других алгоритмов обнаружения аномалий.

Для студентов, обучающихся по направлению подготовки бакалавров и магистров 210700 – «Инфокоммуникационные технологии и системы связи», может быть полезно аспирантам и студентам, обучающимся по группе специальностей направления «Информационная безопасность» и специалистам в области защиты информации и безопасности инфокоммуникаций.

ББК 32.973.2-018.2я73

Учебное издание

Шелухин Олег Иванович, **Сакалема** Домингуш Жайме,
Филинова Анастасия Сергеевна

Обнаружение вторжений в компьютерные сети (сетевые аномалии)
Учебное пособие для вузов

Редактор Ю. Н. Чернышов
Компьютерная верстка Ю. Н. Чернышова
Обложка художника О. Г. Карповой

Подписано к печати 07.02.2013. Формат 60×88 1/16. Усл. печ. л. 13,75. Изд. № 13323. Тираж 500 экз. (1-й завод 200 экз.)

ISBN 978-5-9912-0323-4 © О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова, 2013

© Издательство «Горячая линия–Телеком», 2013

ПРЕДИСЛОВИЕ

Важнейшим атрибутом нашего времени является глобальная информационная интеграция, основанная на построении компьютерных сетей масштаба предприятия и их объединении посредством Интернета.

Сложность логической и физической организации современных сетей приводит к объективным трудностям при решении вопросов управления и защиты сетей. В процессе эксплуатации компьютерных сетей администраторам приходится решать две главные задачи:

- диагностировать работу сети и подключенных к ней серверов, рабочих станций и соответствующего программного обеспечения;
- защищать информационные ресурсы сети от несанкционированной деятельности хакеров, воздействий вирусов, сетевых червей и т. п., т. е. обеспечивать их конфиденциальность, целостность и доступность.

При решении задач, связанных с диагностикой и защитой сетевых ресурсов, центральным вопросом является оперативное обнаружение состояний сети, приводящих к потере полной или частичной ее работоспособности, уничтожению, искажению или утечке информации, являющихся следствием отказов, сбоев случайного характера или результатом получения злоумышленником несанкционированного доступа к сетевым ресурсам, проникновения сетевых червей, вирусов и других угроз информационной безопасности. Раннее обнаружение таких состояний позволит своевременно устранить их причину, а также предотвратит возможные катастрофические последствия.

Для их обнаружения используется большой спектр специализированных систем. Так, при решении проблем диагностики сетей применяются средства систем управления, анализаторы сетевых протоколов, системы нагрузочного тестирования, системы сетевого мониторинга. Проблемы защиты информационных ресурсов сетей решаются с помощью межсетевых экранов (firewall), антивирусов, систем обнаружения атак (COB) (Intrusion Detection System, IDS), систем контроля целостности, криптографических средств защиты.

Характерными особенностями использования этих систем является либо их периодическое и кратковременное применение для решения определенной проблемы, либо постоянное использование, но со статическими настройками. В результате методы анализа, используемые в современных системах, направлены на обнаружение известных и точно описанных типов воздействий, но зачастую оказываются не в состоянии обнаружить их модификации или новые типы, что делает их использование малоэффективным.

Таким образом, на сегодняшний день очень актуальной задачей является поиск более эффективных методов выявления недопустимых событий (аномалий) в работе сети, являющихся следствием технических сбоев или несанкционированных воздействий. Основным требованием к этим методам является возможность обнаружения произвольных типов аномалий, в том числе новых, а также воздействий, распределенных во времени.

Это направление научных исследований является очень молодым. Первые работы, посвященные данной проблеме, были опубликованы в 90-х годах прошлого столетия.

В настоящий момент исследования в этой области ведутся крупными зарубежными коммерческими компаниями. Общий подход, лежащий в основе этих исследований, заключается в поиске методов анализа, позволяющих выявлять аномальные состояния информационных ресурсов в виде отклонений от обычного («нормального») состояния. Эти отклонения могут являться результатами сбоев в работе аппаратного и программного обеспечения, а также следствиями сетевых атак хакеров. Такой подход теоретически позволит обнаруживать как известные, так и новые типы проблем. От эффективности и точности аппарата, определяющего «нормальное» состояние и фиксирующего отклонение, зависит в целом эффективность решения вопросов диагностики и защиты сетевых ресурсов. Особую важность на текущий момент представляет проблема обнаружения аномальных состояний в работе сети, имеющих распределенный во времени характер (АРВ). АРВ могут являться следствиями специально маскируемых сетевых атак злоумышленников, скрытых аппаратно-программных сбоев, новых вирусов и т. п.

В основу учебного пособия положен курс лекционных, практических и лабораторных занятий для студентов МТУСИ, обучающихся по магистерским программам «Программно-защищенные инфокоммуникации» в рамках направлений «Инфокоммуникационные технологии и системы связи», а также «Информатика и вычислительная техника».

Оглавление

Предисловие	3
1. Компьютерные атаки	5
1.1. Основные определения и понятия	5
1.2. Классификация атак	6
1.3. Этапы реализации атак	8
1.3.1. Сбор информации	8
1.3.2. Основные механизмы реализации атак	10
1.3.3. Реализация атак	13
1.3.4. Завершение атаки	14
2. Принципы построения систем обнаружения вторже-	15
ния	15
2.1. Классификация СОВ	15
2.2. Архитектура СОВ	25
2.3. Структура системы обнаружения вторжения	27
3. Технологии построения систем обнаружения атак ...	32
3.1. Существующие технологии СОВ	33
3.1.1. Технологии обнаружения аномальной активности	33
3.1.2. Анализ систем, использующих сигнатурные	
методы	35
3.1.3. Концепция обнаружения компьютерных угроз	38
3.2. Повышение эффективности систем обнаружения атак —	
интегральный подход	42
3.3. Характеристика направлений и групп методов обнару-	
жения вторжений	44
3.4. Сравнительный анализ существующих СОВ	49
3.4.1. Bro	49
3.4.2. OSSEC	50
3.4.3. STAT	51
3.4.4. Prelude	53
3.4.5. Snort	55
3.4.6. SnortNet	58
3.4.7. AAFID	59
4. Анализ сетевого трафика и контента	63

4.1. Программы анализа и мониторинга сетевого трафика	63
4.1.1. Программы-анализаторы сетевого трафика	64
4.1.2. Обзор программ-анализаторов (снифферов) сетевого трафика	67
4.2. Получение и подготовка исходных данных для анализа свойств аномалий трафика	69
4.3. Анализ образцов трафика	71
4.3.1. Трассы и их анализ	73
4.3.2. Тестирование программного обеспечения	74
5. Анализ методов обнаружения аномалий	80
5.1. Статистические методы обнаружения аномального поведения	80
5.2. Ошибки первого и второго рода. ROC кривые	84
5.3. Критерии соответствия и однородности	87
5.4. Параметрический метод регистрации изменений	90
5.4.1. Контрольные карты	91
5.4.2. Контрольные карты Шухарта	93
5.4.3. Контрольные карты CUSUM	94
5.4.4. Контрольные карты EWMA	102
5.5. Критерии аномального поведения и их практическое применение	103
5.5.1. Процентное отклонение	104
5.5.2. Энтропия	108
5.6. Методы описательной статистики	108
5.7. Поиск и оценка аномалий сетевого трафика на основе циклического анализа	110
5.8. Обнаружение аномалий методом главных компонент	121
5.8.1. Основные положения метода главных компонент	121
5.8.2. Сингулярный спектральный анализ	129
5.8.3. Метод главных компонент и обнаружение аномалий	132
5.9. Достоинства и недостатки статистических методов	135
6. Обнаружение аномальных выбросов трафика методами кратномасштабного анализа	138
6.1. Основы теории вейвлетов	138
6.2. Непрерывное вейвлет-преобразование	139
6.3. Дискретное вейвлет-преобразование. Алгоритм Малла	141
6.4. Анализ методов обнаружения аномалий трафика с помощью вейвлетов	147

6.5. Алгоритм обнаружения аномалий методом дискретного вейвлет-преобразования	150
6.5.1. Алгоритм обнаружения аномалий по критерию Фишера для выбросов дисперсий	151
6.5.2. Алгоритм обнаружения аномалий на основе критерия Кохрана-Кокса	152
6.5.3. Алгоритм обнаружения аномалий по критерию Фишера для выбросов средних значений	153
6.5.4. Выбор порогов обнаружения	155
6.6. Дискретное вейвлет-пакетное преобразование	156
6.7. Обнаружение DoS- и DDoS-атак методами мультифрактального анализа	162
6.7.1. Фрактальные свойства телекоммуникационного трафика	162
6.7.2. Обнаружение DoS- и DDoS-атак методом мультифрактального анализа	166
7. Методы интеллектуального анализа данных в системах обнаружения вторжений	172
7.1. Методы Data Mining	172
7.2. Метод опорных векторов	175
7.3. Обнаружение аномалий трафика с применением нейронных сетей	182
7.3.1. Выявление аномалий сетевой активности с применением аппарата искусственных нейронных сетей	183
7.3.2. Применение нейронных сетей в задачах обнаружения вторжений	186
7.3.3. Архитектурные решения COB	187
7.3.4. Результаты экспериментов	190
7.4. Методы искусственного интеллекта в задачах обеспечения безопасности компьютерных сетей	192
7.4.1. Многоагентные системы	192
7.4.2. Системы анализа защищенности	193
7.5. Методы искусственных иммунных систем и нейронных сетей для обнаружения компьютерных атак	195
7.5.1. Построения искусственной иммунной системы для обнаружения компьютерных атак	195
7.5.2. Метод функционирования иммунных нейросетевых детекторов	197
7.5.3. Алгоритм функционирования системы обнаружения вторжений на базе искусственных иммунных систем и нейронных сетей	201
7.6. Визуальный анализ данных	203
7.6.1. Анализ методов визуализации	203

7.6.2. Использование преобразования Хафа для обнаружения аномалий трафика	207
7.7. Достоинства и недостатки методов обнаружения аномалий	209
Литература	212